Getting Started with the SCAP Compliance Checker and STIG Viewer

1 SCAP Compliance Checker

The SCAP Compliance Checker is an automated vulnerability scanning tool that leverages the DISA Security Technical Implementation Guidelines (STIGs) and operating system (OS) specific baselines to analyze and report on the security configuration of an information system. The tool can be run locally on the host system to be scanned, or scans can be conducted across a network from any machine on the domain. In either scanning environment, the following requirement applies: The user conducting the scan must have administrative privileges on the machine to be scanned. If the machine to be scanned is not hosting the tool, domain-level administrative privileges (or individual local administrator accounts) are required to remotely scan other systems on the network.

1.1 Obtaining the SCAP Tool

The SCAP Compliance Checker can be obtained in two ways, depending upon the possession of a DoD PKI token:

1.1.1 PKI enabled:

- Navigate to DISA's Information Assurance Support Environment (IASE) webpage at the following URL: http://iase.disa.mil/stigs/scap/Pages/index.aspx , and scroll to the bottom section titled "SCAP Tools".
- Identify the appropriate version of the tool that corresponds to the Operating System that will host the application, and provide your PKI credentials when prompted to start the download of the ZIP file.

1.1.2 Non-PKI Enabled:

Navigate to the MAX.gov website, administrated by the Office of Management and Budget and complete the process to create a user account:

- Register a user account with MAX.gov
  - If you are a federal government employee or federal government contractor with a government email address, no extra steps are necessary.

- If you do not have a federal government email address, please contact MAXSupport@omb.eop.gov or call 202-395-6860. Upon providing proof that you are supporting a federal government program (e.g. Contract Number) you will be allowed to create an unrestricted account.

- Once logged in to the MAX.gov homepage, search for "SCAP", or Click Here to be taken to the SCAP landing page.
- Scroll to the bottom section and identify the appropriate version of the tool that corresponds to the Operating System that will host the application, and then download the ZIP file.

1.2 Installing the SCAP Compliance Checker:

Within the ZIP file for each Operating System version of the SCAP Compliance Checker is an included PDF, instructing the user on the appropriate way to install and configure the software executable on the host system. The user will need to be logged onto the system as an Administrator in order for the package to install correctly.

1.3 Running the SCAP tool and Exporting Scan Results:

Please refer to the SCAP Tool Instruction Guide included with the downloaded SCAP software package for instructions on how to run scans, save scan results, and export scan results for use in the STIG Viewer.

2 STIG Viewer

The STIG Viewer is a Java-based application that will be used in conjunction with the SCAP Compliance Checker scan results in order to view the compliance status of the system's security settings. The STIG Viewer can also be used in a manual fashion (e.g. without SCAP tool results) to conduct a manual audit of information system security controls. Use of the viewer does not require administrator privileges, provided that the required software packages to support Java applications have been installed on the system.

2.1 Obtaining the DISA STIG Viewer (Version 2.2)

The DISA STIG Viewer is an unclassified, non-PKI controlled tool that can be accessed and downloaded on DISA's IASE website at the following URL: http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

The tool requires no installation, and runs as a Java applet from any directory on the host machine.

3 Operating System Baselines

The STIG Viewer leverages operating System baselines to generate checklists used for vulnerability assessments. These baselines are version- specific, so ensure that you download the appropriate baseline for the operating system you wish to assess. For purposes of viewing scan results of machines other than the host machine, download the baseline representing the scanned system's architecture. The baselines are unclassified; non-PKI controlled, and can be downloaded by navigating to DISA's IASE website at the following URL: http://iase.disa.mil/stigs/os/Pages/index.aspx